

REMARKS

The following Request for Reconsideration is submitted in response to the Office Action issued on November 2, 2004 (Paper No. unknown) in connection with the above-identified patent application, and is being filed within the three-month shortened statutory period set for a response by the Office Action.

Claims 1-46 are pending in the present application, and stand rejected. Applicants respectfully request reconsideration and withdrawal of the rejection of the claims, consistent with the following remarks.

As set forth in the present application, the present invention is directed toward the problem that for a computing device such as a portable computing device to be trusted in the context of a rights management architecture, the portable device and the processor thereon must be of a type that substantially completely prevents a content thief from performing nefarious acts that would allow obtaining of content therein in an unencrypted form or decryption keys. Thus, according to the present invention, the processor is a secure processor and is constructed to run only authorized code, and is operated to maintain a strict cryptographic separation between applications that may be instantiated thereon.

Generally, in the present invention, the security of the processor is based on the use of a security kernel in the processor. Such security kernel provides relevant higher-level functionality including protection from hostile code (e.g. a virus), authentication to a remote host, certification of upgrades, and piracy protection for software on the portable device. Significantly, the secure processor is constructed to include a security (CPU) key physically hard-wired (permanently stored) thereinto, and the security kernel is also physically hard-wired thereinto, where only the security kernel can access the CPU key. Also

significantly, the secure processor is operable in a normal mode and a preferred mode, where the security kernel can access the CPU key only during the preferred mode. The security kernel employs the accessed CPU key during the preferred mode to instantiate and/or authenticate a secure application such as a rights management system, a banking / financial system, etc. on the portable device. The security kernel may automatically instantiate a particular secure application, may authenticate a secure application instantiated by another process, or may initially instantiate a secure chooser application that allows a user to select from one or more available secure applications on the portable device.

In any case, the accessed CPU key is typically a symmetric key that is employed by the security kernel to decrypt one or more encrypted security keys for the application instantiated. For example, in the case where the security kernel instantiates / authenticates the a rights management system on the portable device, it may be that at least the private key (PR) for the rights management system is already encrypted according to the CPU key and stored on the portable device as CPU(PR), and the security kernel during the preferred mode employs the accessed CPU key to decrypt CPU(PR) to produce (PR) such that (PR) is available to the instantiated rights management system. Thus, the CPU key as accessible only by the security kernel and only during the preferred mode is the key to unlocking or decrypting the secrets identified with each application, and therefore must be well-protected.

The Examiner has rejected claims 28 and 44 under 35 USC § 102(b) as being anticipated by Marino, Jr. et al. (U.S. Patent No. 5,029,206). Applicants respectfully traverse the § 102(b) rejection of such claims.

Independent claim 28 of the present application recites a method for a secure processor to instantiate a secure application thereon. In the method, a first security kernel is instantiated which employs symmetric cryptography, and a second security kernel is instantiated by way of the instantiated first security kernel, where the second security kernel employs asymmetric cryptography. Finally, the instantiated second security kernel authenticates the secure application.

Independent claim 44 recites the subject matter of claim 28, albeit in the form of a computer-readable medium. Thus, and as may be appreciated, the second security kernel is the 'instantiated application' with regard to the first security kernel, and is to be employed in the instance where the recited application requires authentication according to an asymmetric cryptography algorithm.

The Marino reference discloses a security kernel for a secure processing system where the kernel interfaces between a red (plain text) sub-system and a black (encoded text) sub-system, and thus employs appropriate keys and protocols to transfer text between the sub-systems as plain and encoded forms. In addition, the Marino security kernel is disclosed as performing ministerial function including key management, re-keying, and the like. Significantly, and as should be appreciated, the Marino security kernel is not disclosed as being employed to instantiate an application, as is required by the claims of the present application, but instead is employed to encrypt and decrypt text.

Also significantly, the Marino security kernel is a single security kernel and is thus not a first kernel that instantiates a second kernel or a second kernel as instantiated by a first kernel, as is required by claims 28 and 44. At any rate, the Marino reference does not disclose a first kernel performing symmetric cryptography and a second kernel performing

asymmetric cryptography and instantiated by the first kernel, as is also required by claims 28 and 44.

Thus, Applicants respectfully submit that the Marino reference does not disclose the subject matter recited in independent claims 28 and 44 or any claims depending therefrom. Accordingly, Applicants respectfully submit that the Marino reference cannot be applied to anticipate such claims. Thus, Applicants respectfully request reconsideration and withdrawal of the § 102(b) rejection.

The Examiner has rejected claims 1-2, 4, 6, 7, 9-20, 27, 31-36, and 46 (although it is believed that 46 should in fact be 43) under 35 USC § 103(a) as being obvious over the Marino reference in view of Angelo et al. (U.S. Patent No. 6,581,162). Applicants respectfully traverse the first § 103(a) rejection of such claims.

Independent claim 15 of the present application recites a method for a secure processor to instantiate and authenticate a secure application thereon by way of a security kernel. In the method, the secure processor enters a preferred mode where a security key of the processor is accessible and instantiates and runs a security kernel. Thereafter, the security kernel accesses the security key and applies same to decrypt at least one encrypted key for the application, stores the decrypted key(s) in a location where the application will expect the key(s) to be found, and authenticates the application on the processor. The secure processor then enters a normal mode from the preferred mode after the security kernel authenticates the application, where the security key is not accessible. Thus, the security kernel allows the processor to be trusted to keep hidden the key(s) of the application.

Independent claim 31 recites the subject matter of claim 15, albeit in the form of a computer-readable medium, and independent claim 31 recites the subject matter of claim 15, albeit in the form of the secure processor.

Applicants respectfully submit that the Marino security kernel is not employed to instantiate and authenticate a secure application on a secure processor, as is required by claims 1, 15, and 31. In particular, Applicants respectfully submit that the Marino kernel is not disclosed or suggested as accessing a security key in a preferred mode and applying same to decrypt at least one encrypted key for an application, storing the decrypted key in a location where the application will expect the key to be found, and authenticating the application on the processor, as is also required by claims 1, 15, and 31. In fact, inasmuch as the Marino kernel is employed primarily to encrypt and decrypt text, the Marino kernel is not disclosed or suggested as providing any key for any Marino application or authenticating any such application, as is required by claims 1, 15, and 31.

As the Examiner concedes, the Marino reference does not teach a security processor that is operated in a normal mode and a preferred mode, where a security key is accessible to a security kernel operating on the processor only when such processor is in the preferred mode and not in the normal mode. Nevertheless, the Examiner argues that such modes are set forth in the Angelo reference.

In fact, the Angelo reference discloses a computer system that operates in normal and secure modes. In the normal mode, normal processes and operations are performed, while in the secure mode secure processes and operations are performed, including encryption and decryption processes. Significantly, though, the Angelo reference does not disclose or suggest that the secure mode be employed to decrypt at least one

encrypted key for an application, store the decrypted key in a location where the application will expect the key to be found, and authenticate the application, as is required by claims 1, 15, and 31. Instead, the Angelo secure mode appears to be employed only to encrypt and decrypt user passwords for a user of the Angelo computer system.

Accordingly, Applicants respectfully submit that the combination of the Marino and Angelo references does not disclose or even suggest the invention recited in claims 1, 15, and 31 or any claims depending therefrom. As a result, such Marino and Angelo references cannot be combined to make obvious such claims or any claims depending therefrom, including claims 2, 4, 6, 7, 9-14, 16-20, and 32-36.

With regard to claims 27 and 43, Applicants respectfully point out that such claims depend from independent claims 25 and 41, and that claims 25 and 41 stand rejected under section 103 as being obvious over the Marino and Angelo references and further in view of Downs et al. (see below). Accordingly, based on such dependency, such claims 27 and 43 cannot be rejected under section 103 on any basis that does not include such Downs reference. As a result, the obviousness rejection of such claims 27 and 43 as set forth in the Office Action should be withdrawn for this reason alone.

Thus, Applicants respectfully request reconsideration and withdrawal of the first § 103(a) rejection.

The Examiner has rejected claims 3, 5, 21-26, 29-30, 37-42, and 45-46 under 35 USC § 103(a) as being obvious over the Marino reference in view of the Angelo reference and further in view of Downs et al. (U.S. Patent No. 6,574,609). Applicants respectfully traverse the second § 103(a) rejection of such claims.

With regard to claims 3, 5, 21-24, 29-30, 37-40, and 45-46 Applicants respectfully point out that since independent claims 1, 15, 28, 31, and 44 have been shown to be unanticipated and non-obvious, then so too must all claims depending therefrom be unanticipated and non-obvious, including such claims 3, 5, 21-24, 29-30, 37-40, and 45-46, at least by their dependencies.

With regard to claims 25, 26, 41, and 42, independent claim 25 recites a method for a secure processor to instantiate one of a plurality of available secure applications thereon by way of a security kernel. In the method, a chooser value is set to a value corresponding to a chooser application upon power-up, and a preferred mode is entered upon a power-up CPU reset and instantiating the security kernel. The security kernel determines that the chooser value corresponds to the chooser application and therefore authenticates and instantiates same.

After the chooser application is instantiated, a normal mode is entered and the chooser application presents the plurality of available applications for selection by a user. Upon receiving a selection of one of the presented applications to be instantiated, the chooser value is set to a value corresponding to the selected application. Thereafter, a CPU reset is executed and the preferred mode is entered, and the security kernel is instantiated. The security kernel then determines that the chooser value corresponds to the selected application and therefore authenticates and instantiates same. Normal mode is then entered after the selected application is instantiated and run. Thus, the security kernel allows the processor to be trusted to keep hidden a secret of the chooser application and a secret of the selected application.

Independent claim 41 recites the subject matter of claim 25, albeit in the form of a computer-readable medium.

As the Examiner concedes, the Marino and Angelo references do not disclose or suggest any such chooser application or process by which such chooser application and a chooser value is employed. Nevertheless, the Examiner argues that the Downs reference supplies such items.

The Downs reference discloses a method of managing content data and associated metadata. According to the method, content data is encrypted with a first encrypting key before being transferred to a content host, the first encrypting key is encrypted with a second encrypting key, and the encrypted first encrypting key is transferred along with metadata and usage condition data to an the electronic store. Although the Examiner argues that the Downs reference discloses use of a chooser value and a chooser application, Applicants quite frankly cannot find within the cited portions of the Downs reference such items. Moreover, Applicants respectfully submit that none of the Marino, Angelo, and Downs references, alone or combined, discloses or suggests all of the many steps recited in claims 25 and 41, including switching between the modes as recited to first load and then operate the chooser application, employing same to select a chooser value corresponding to a chosen application, and then loading and operating the chosen application.

Thus, Applicants respectfully submit that the combination of the Marino, Angelo, and Downs references does not disclose or suggest the subject matter recited in independent claims 25 and 41 or any claims depending therefrom, including claims 26 and 42. Accordingly, and for all the aforementioned reasons, Applicants respectfully submit that the aforementioned references cannot be applied to make obvious such claims.

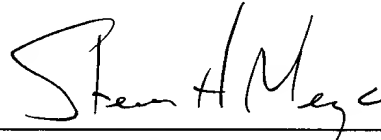
DOCKET NO.: MSFT-0312/164268.1
Application No.: 09/892,329
Office Action Dated: November 2, 2004

PATENT

Thus, Applicants respectfully request reconsideration and withdrawal of the second § 103(a) rejection.

In view of the foregoing discussion, Applicants respectfully submit that the present application, including claims 1-46, is in condition for allowance, and such action is respectfully requested.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Steven H. Meyer", is written over a horizontal line.

Steven H. Meyer
Registration No. 37,189

Date: January 31, 2004

Woodcock Washburn LLP
One Liberty Place - 46th Floor
Philadelphia PA 19103
Telephone: (215) 568-3100
Facsimile: (215) 568-3439